I.T.I.S. & L.S.
F. GIORDANI
TEC LIM

ITIS-LS "Francesco Giordani" Caserta

prof. Ennio Ranucci

a.s. 2019-2020

Privacy

GESTIONE DELLA PRIVACY E DEI DATI SENSIBILI

Aristotele faceva distinzione tra la sfera pubblica (annessa all'attività politica) e la sfera privata (annessa alla attività familiare). I messaggi militari venivano cifrati come quelli amorosi.
La tutela del dato iniziava a prendere forma. Il flusso dei dati, in chiaro, o le informazioni venivano quindi fatte circolare attraverso un numero ristretto di persone (tribù, villaggi, famiglie, eserciti). Ricordiamo il famoso cifrario di Cesare, con il quale crittografava gli ordini ai suoi generali; il dato non doveva finire in mani ostili o non autorizzate. Oppure la scacchiera di Polibio, sistema crittografico dal famoso storico greco verso il 150 a.C., descritto nelle sue Storie che si basava sul frazionamento dei caratteri del messaggio in chiaro così che potessero essere rappresentati utilizzando un più piccolo insieme di simboli.

Proseguendo nel cammino del tempo arriviamo al medioevo dove i messaggi segreti (militari e non) proliferavano e dove il termine privato divenne sinonimo di familiare; infatti la vita privata era basata sulla fiducia reciproca che univa i membri del gruppo dando luogo ad una vita familiare intesa in senso conviviale, dove non vi era spazio per l'individuo. Ecco che allora inizia a prendere forma la necessità di appartarsi, di avere intimità in tutti i campi (religioso, sociale di pensiero) di vivere a stretto contatto con i familiari e gli amici più cari. Inizia a nascere il concetto di riservatezza che si avvicina a quello dei giorni nostri. L'individuo riscopre se stesso come entità singola.
L'inizio della storia del diritto alla privacy è nell'articolo "Right to privacy", apparso il 15 dicembre 1890 sulla Harvard Law Review (che è tuttora la più famosa rivista giuridica degli Stati Uniti), ad opera di due giovani avvocati bostoniani, Samuel D. Warren e Louis D. Brandeis, i quali analizzarono in maniera molto precisa e articolata il rapporto tra il diritto di informare ed essere informati e la riservatezza.
In Europa, diversamente dagli Stati Uniti, si è verificata una storia di stati totalitari, che hanno agito da "super-controllori" nei confronti dei cittadini: per tale ragione, in Europa si è sviluppata, dal punto di vista storico, una sensibilità diversa nei confronti della privacy.
La Convenzione europea dei diritti dell'uomo (CEDU), firmata a Roma il 4 novembre 1950 sotto l'egida del Consiglio d'Europa (composto nel 1950 da 12 stati membri, oggi ne conta 47), ha creato un sistema di tutela internazionale dei diritti dell'uomo. La Convenzione, successivamente ratificata da tutti gli Stati membri dell'UE, ha istituito diversi organi di controllo, insediati a Strasburgo, sostituti il 1 novembre 1998 da un'unica Corte europea dei diritti dell'uomo. Nella storia europea della protezione dei dati personali, in una prima fase la CEDU ha avuto un ruolo di primaria importanza, perché prima ancora che fossero istituite le prime comunità europee, fra i diritti fondamentali previsti nella CEDU (testo integrale tradotto in italiano) ce n'è uno, l'art. 8, nell'ambito del quale già emerge il diritto alla riservatezza:
Art. 8 - Diritto al rispetto della vita privata e familiare
1. Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.
2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui.
In sostanza, la CEDU dice che ogni persona ha diritto al rispetto della propria vita privata e di quella della propria famiglia, e che questo diritto si impone anche all'autorità pubblica, che può entrare nella vita privata degli individui e delle famiglie solo se è strettamente necessario e previsto dalla legge (praticamente il contrario di quel che a quel tempo stava accadendo nei paesi europei rimasti ad Est, l'Europa era spaccata in due dalla "cortina di ferro").

Il regolamento Privacy, meglio noto come Gdpr, è stato pubblicato in Gazzetta Ufficiale con il Decreto n.101/18 del 10 agosto 2018, ufficialmente in vigore 19 settembre 2018.

Così anche l'Italia si deve adeguare al regolamento europeo che detta nuove norme precise sulla privacy dei cittadini europei: Il General data protection regulation

In Italia c'era già il decreto legislativo n. 196 del 2003, intitolato "Codice in materia di Protezione dei dati personali", meglio conosciuto come Codice della Privacy che prevede degli specifici obblighi per coloro che sono in possesso di informazioni personali riguardanti altri soggetti, e dei corrispondenti diritti a favore dei soggetti cui i dati si riferiscono. Il Codice della Privacy prevede delle modalità di trattamento dei dati che sono tanto più incisive quanto più delicate sono le informazioni che ne formano oggetto.

E' proprio per questo motivo che tutte le volte che ci troviamo a comunicare i nostri dati personali a terzi (si pensi, per esempio, al momento dell'apertura di un conto corrente presso una banca o anche a quello dell'apertura di un account in un social network) ci si chiede di prendere visione e firmare la cosiddetta privacy policy dove si richiede il nostro consenso all'utilizzo dei nostri dati personali per le finalità connesse al servizio richiesto.

Il Codice della Privacy definisce trattamento qualunque operazione concernente "la raccolta, la registrazione, l'organizzazione, la conservazione, la consultazione, l'elaborazione, la modificazione, la selezione, l'estrazione, il raffronto, l'utilizzo, l'interconnessione, il blocco, la comunicazione, la diffusione, la cancellazione e la distruzione di dati, anche se non registrati in una banca di dati" (art. 4).

Pertanto, tutte le volte in cui in cui ci vengono richiesti dati personali, chi che li riceve è tenuto ad osservare determinate procedure definite modalità di trattamento dei dati.

Il primo obbligo per chi richiede dati personali è di dare all'interessato un'informativa (art. 13 Codice della Privacy).

Tutti i soggetti che intendono effettuare un trattamento di dati personali devono prima fornire all'interessato alcune informazioni per metterlo nelle condizioni di esercitare i propri diritti.

Cosa deve contenere l'informativa per essere legale?

In particolare, l'informativa alla privacy deve indicare:
chi è l'interessato, cioè il soggetto al quale il dato si riferisce, e quali sono i suoi diritti; quali dati vengono trattati;
in che modo, per quale scopo e per quanto tempo verranno trattati i propri dati personali;
qual è la base giuridica del trattamento;
se il conferimento dei propri dati personali è obbligatorio o facoltativo;
le conseguenze di un eventuale rifiuto a rendere disponibili i propri dati personali;
se saranno diffusi a terzi i propri dati personali e a chi; chi è il titolare del trattamento;
chi è il responsabile del trattamento;
Se nominato, i recapiti del DPO.
Questa informativa deve essere sottoscritta dal legittimo interessato.
Non è possibile conservare né tanto meno diffondere dati personali senza il consenso del legittimo interessato.

Dati personali

I dati personali sono quelli idonei a dare informazioni inerenti la propria persona (nome, cognome, indirizzo, data di nascita, residenza, titolo di studio) e che non rientrano in quelli sensibili.
Per questi tipi di dati l'interessato ha diritto di ottenere conferma della esistenza o meno di dati che lo riguardano con l'indicazione dei medesimi (art. 7 d. lgs. n. 196/2033). Ha diritto ad ottenere l'aggiornamento, la rettificazione o, quando vi ha interesse, l'integrazione che ritiene o la cancellazione o la trasformazione in forma anonima: in ogni caso i dati stessi devono essere trattati in modo lecito e secondo specifiche regole che si possono definire di correttezza. Essi devono essere espliciti, legittimi, esatti, aggiornati, pertinenti, completi e non eccedenti rispetto alla finalità dichiarata.

Dati sensibili

I dati sensibili sono quei dati idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche e di ogni altro genere, le opinioni politiche, l'adesione a partiti, sindacati associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale (art. 4 del Codice della Privacy).

Si ha violazione del diritto alla privacy tutte le volte in cui:

non viene data l'informativa di cui all'art. 13 del Codice della Privacy;
oppure quando l'informativa in questione non contiene tutti i dati indicati dalla legge;
i dati vengono trattati secondo modalità diverse da quelle indicate dalla legge o nell'informativa (ad es. sono conservati per un tempo più lungo di quello dichiarato); i dati vengono diffusi a terzi senza il consenso dell'interessato.

Il GDPR ha introdotto importanti novità in materia di Privacy e ha introdotto sanzioni più severe per i trasgressori.

Le principali novità introdotto con il Regolamento sono:
ha introdotto il dovere di documentazione di tutti i trattamenti di dati effettuati;
ha reso più semplice l'informativa di cui all'art. 13 (prima infatti le informative erano piuttosto complicate e risultava difficile per l'utente comprenderla);
il consenso prestato deve essere libero e inequivocabile;
ha introdotto la figura del Data Protection Officer (DPO), concepito come il soggetto responsabile della protezione dei dati. Gli Enti pubblici e le aziende sono obbligate a nominarlo; ha introdotto sanzioni più severe in caso di violazione.

Educare all'uso delle nuove tecnologie.

Internet Security Policy è l'acronimo usato per descrivere le attuali politiche atte a favorire la sicurezza del sistema internet. Con politiche si intende l'insieme di accorgimenti procedurali, siano essi inseriti in un quadro legislativo o consuetudinale, che hanno lo scopo di permettere il sicuro utilizzo, in questo caso, della rete. Tra le politiche intraprese dalla comunità cybernetica, grande importanza rivestono i cosiddetti Standard di sicurezza informatica, che sono metodologie che permettono alle organizzazioni di attuare tecniche di sicurezza finalizzate a minimizzare la quantità e la pericolosità delle minacce alla sicurezza informatica. L'obiettivo principale della sicurezza è quello di garantire, riducendo i rischi, un adeguato grado di protezione dei beni o dati.

Il codice in materia di protezione dei dati personali è un decreto legislativo (atto avente forza di legge) della Repubblica Italiana emanato il 30 giugno 2003, al n. 196 e noto comunemente anche come «Testo unico sulla privacy».
Sull'applicazione della normativa vigila l'Autorità Garante per la protezione dei dati personali, istituita sin dalla L. 675/1996, poi confermata anche dal Testo Unico del 2003.

Il diritto alla privacy è riconosciuto come un diritto fondamentale delle persone, direttamente collegato alla tutela della dignità umana, ed è sancito anche dalla Carta dei diritti fondamentali dell'Unione Europea.

Il concetto di privacy, parola inglese traducibile in italiano con "riservatezza" o "privatezza", con il tempo si è evoluto: dal diritto "di essere lasciati in pace o di proteggere la propria sfera privata", oggi nella società dell'informazione, si riferisce soprattutto al diritto di accedere e controllare l'uso e la circolazione dei propri dati personali.

I DATI PERSONALI
"dati identificativi": le informazioni che identificano o rendono identificabile una persona fisica, come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc.;

"dati sensibili": quelli che possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;

"dati giudiziari": quelli che possono rivelare l'esistenza di determinati provvedimenti giudiziari soggetti ad iscrizione nel casellario giudiziale (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

Con l'evoluzione delle nuove tecnologie, altri dati personali hanno assunto un ruolo significativo, come quelli relativi alle comunicazioni 9elettroniche (via Internet o telefono) e quelli che consentono la geolocalizzazione, fornendo informazioni sui luoghi frequentati e sugli spostamenti.

PER I DATI SENSIBILI NON BASTA IL CONSENSO ORALE

II trattamento di dati personali da parte di privati o di enti pubblici economici è ammesso solo con il consenso espresso dell'interessato.

Particolare attenzione, e una maggiore protezione, sono rivolte ai dati sensibili, infatti il consenso al trattamento dei dati sensibili da parte dell'interessato deve essere reso sempre in forma scritta (o con firma elettronica).

Ma per il principio di necessità del trattamento dei dati, il dato, per essere trattato, deve essere funzionale al tuo fine (dichiarato nell'informativa).

Se tu vendi fiori ad un tuo cliente che senso ha chiedergli il titolo di studio, quello dei genitori e semmai la sua situazione patrimoniale?

Ma lui mi ha autorizzato!

Si, lui si, ma è la legge che non ti autorizza!

La privacy a scuola

Temi in classe

Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi in classe riguardanti il loro mondo personale. Sta invece nella sensibilità dell'insegnante, nel momento in cui gli elaborati vengono letti in classe, trovare l'equilibrio tra esigenze didattiche e tutela della riservatezza, specialmente se si tratta di argomenti delicati.

Recite e gite scolastiche

Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici. Le immagini in questi casi sono raccolte a fini personali e destinati ad un ambito familiare o amicale. Nel caso si intendesse pubblicarle e diffonderle in rete, anche sui social network, è necessario ottenere di regola il consenso delle persone presenti nei video o nelle foto.

Voti, scrutini, esami di Stato

I voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato sono pubblici. Le informazioni sul rendimento scolastico sono soggette ad un regime di trasparenza e il regime della loro conoscibilità è stabilito dal Ministero dell'istruzione. E' necessario però, nel pubblicare voti degli scrutini e degli esami nei tabelloni, che l'istituto eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti: il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap, ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.